Journal of Computational and Applied Mathematics 37 (1991) 19–25
North-Holland

Some congruences and identities for Gauss polynomials: a noncommutative technique

Christian Radoux

Institut de Mathématique et d'Informatique, Faculté des Sciences, Université de Mons-Hainaut, Avenue Maistriau 15, B-7000 Mons, Belgium

Received 7 October 1989

Abstract

Radoux, C., Some congruences and identities for Gauss polynomials: a noncommutative technique, Journal of Computational and Applied Mathematics 37 (1991) 19–25.

Gauss polynomials are used to obtain a generalization (involving cyclotomic polynomials) of the congruence of Lucas. We give two proofs of this statement. The second one contains a noncommutative q-analogue of Newton's formula. The paper ends with some applications (identities and congruences). For instance, $(\Phi_n(q))^2$ divides $\begin{bmatrix} 2n \\ n \end{bmatrix}_q - 1 - q^{(n^2)}$.

Keywords: Gauss polynomials, cyclotomic polynomials, noncommutative algebra, congruence of Lucas.

1. Definition and elementary properties

Gauss polynomial $\begin{bmatrix} m \\ n \end{bmatrix}_q$ is defined, when $0 < n < m$, by

$$\begin{bmatrix} m \\ n \end{bmatrix}_q = \begin{cases} \dfrac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-n+1}-1)}{(q-1)(q^2-1)\cdots(q^n-1)}, & \text{if } q \neq 1, \\ \binom{m}{n}, & \text{if } q = 1 \text{ (for the sake of continuity).} \end{cases} \tag{1}$$

We put also

$$\begin{bmatrix} m \\ 0 \end{bmatrix}_q = \begin{bmatrix} m \\ m \end{bmatrix}_q = 1 \tag{2}$$

and

$$\begin{bmatrix} m \\ n \end{bmatrix}_q = 0, \quad \text{when } n > m. \tag{3}$$

It is well known (and obvious) that

$$\begin{bmatrix} m \\ m-n \end{bmatrix}_q = \begin{bmatrix} m \\ n \end{bmatrix}_q \tag{4}$$

and

$$\begin{bmatrix} m \\ n \end{bmatrix}_q = \begin{bmatrix} m-1 \\ n \end{bmatrix}_q + q^{m-n} \begin{bmatrix} m-1 \\ n-1 \end{bmatrix}_q. \tag{5}$$

In one of his proofs of the law of quadratic reciprocity, Gauss gave the beautiful formula

$$\sum_{n=0}^{m} q^n \begin{bmatrix} m \\ n \end{bmatrix}_{q^2} = \prod_{j=1}^{m} (1+q^j). \tag{6}$$

2. Main theorem

Let us recall the theorem of E. Lucas.

Theorem. *If p is a prime and if the p-ary expansion of*

$$\begin{Bmatrix} m \\ n \end{Bmatrix} \quad is \quad \begin{cases} \sum_{i=0}^{k} m_i p^i, \\ \sum_{i=0}^{k} n_i p^i, \end{cases}$$

then

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}. \tag{7}$$

We give two proofs of the following similar statement. If $m = ka + b$ and $n = kc + d$, where $0 \leqslant b < k$, $0 \leqslant d < k$, then

$$\begin{bmatrix} m \\ n \end{bmatrix}_q \equiv \binom{a}{c} \begin{bmatrix} b \\ d \end{bmatrix}_q \pmod{\Phi_k(q)\mathbb{Z}[q]}, \tag{8}$$

where Φ_k is the kth cyclotomic polynomial.

3. First proof (Radoux [2])

Let us show first that

$$\frac{\prod_{t=1}^{m} (1-q^t)}{(1-q^k)^a} \equiv k^a a! \prod_{t=1}^{b} (1-q^t) \pmod{\Phi_k(q)\mathbb{Z}[q]}. \tag{9}$$

We can write indeed

$$\prod_{t=1}^{n} (1-q^t) = \left(\prod_{r=0}^{a-1} \prod_{t=1}^{k-1} (1-q^{kr+t}) \right) \left(\prod_{t=1}^{a} (1-q^{kt}) \right) \left(\prod_{t=1}^{b} (1-q^{ka+t}) \right). \tag{10}$$

But $q^k - 1 = \prod_{t|k} \Phi_t(q)$. Therefore $q^k \equiv 1 \pmod{\Phi_k(q)\mathbb{Z}[q]}$ and

$$\prod_{t=1}^{b} (1 - q^{ka+t}) \equiv \prod_{t=1}^{b} (1 - q^t) \pmod{\Phi_k(q)\mathbb{Z}[q]}, \tag{11}$$

$$\prod_{t=1}^{k-1} (1 - q^{kr+t}) \equiv \prod_{t=1}^{k-1} (1 - q^t) \pmod{\Phi_k(q)\mathbb{Z}[q]}. \tag{12}$$

Now, if α is any kth primitive root of unity, we have

$$\prod_{t=1}^{k-1} (1 - \alpha^t) = \left\{ \prod_{t=1}^{k-1} (x - \alpha^t) \right\}_{x=1} = \left\{ \frac{x^k - 1}{x - 1} \right\}_{x=1} = \left\{ \sum_{t=0}^{k-1} x^t \right\}_{x=1} = k.$$

But $\Phi_k(q) = \prod_{\alpha}(q - \alpha)$. So we have

$$\prod_{t=1}^{k-1} (1 - q^t) \equiv k \pmod{\Phi_k(q)\mathbb{Z}[q]} \tag{13}$$

and (12) becomes

$$\prod_{t=1}^{k-1} (1 - q^{kr+t}) \equiv k \pmod{\Phi_k(q)\mathbb{Z}[q]}. \tag{14}$$

On the other hand, it is obvious that $(1 - q^k)^a$ divides $\prod_{t=1}^{a}(1 - q^{kt})$. Thus, if α denotes always any kth primitive root of 1,

$$\lim_{q \to \alpha} \frac{\prod_{t=1}^{a} (1 - q^{kt})}{(1 - q^k)^a} = \lim_{q^* \to 1} \frac{\prod_{t=1}^{a} (1 - q^{*t})}{(1 - q^*)^a} \quad (\text{where } q^k = q^*)$$

$$= \lim_{q^* \to 1} \prod_{t=1}^{a} \left(\frac{1 - q^{*t}}{1 - q^*} \right) = a!.$$

Using again $\Phi_k(q) = \prod_{\alpha}(q - \alpha)$, we get

$$\frac{\prod_{t=1}^{a} (1 - q^{kt})}{(1 - q^k)^a} \equiv a! \pmod{\Phi_k(q)\mathbb{Z}[q]} \tag{15}$$

and (9) is now well established. Formula (8) follows at once if we remember definition (1).

4. Second proof

A q-analogue of Newton's formula. *Let $\mathscr{A}$ be an associative, noncommutative algebra and $A, B \in \mathscr{A}$ such that*

$$BA = qAB, \tag{16}$$

where q commutes with A and B. Then

$$\forall m \in \mathbb{N}, \ (A + B)^m = \sum_{n=0}^{m} \begin{bmatrix} m \\ n \end{bmatrix}_q A^n B^{m-n}. \tag{17}$$

Proof (*by induction on m*). (a) For $m = 0$, the two members of (17) reduce to 1.

(b) If (17) is true for $m = p$, then

$$\begin{aligned}(A+B)^{p+1} &= (A+B)^p(A+B)\\ &= \left(\sum_{n=0}^{p}\begin{bmatrix}p\\n\end{bmatrix}_q A^n B^{p-n}\right)(A+B)\\ &= \sum_{n=0}^{p}\begin{bmatrix}p\\n\end{bmatrix}_q A^n B^{p-n}A + \sum_{n=0}^{p}\begin{bmatrix}p\\n\end{bmatrix}_q A^n B^{p+1-n}.\end{aligned}$$

But

$$\begin{aligned}A^nB^{p-n}A &= A^nB^{p-n-1}BA = qA^nB^{p-n-1}AB \quad \text{(because of (16))}\\ &= qA^nB^{p-n-2}BAB = q^2A^nB^{p-n-2}AB^2\\ &= \cdots\\ &= q^{p-n}A^nAB^{p-n}\\ &= q^{p-n}A^{n+1}B^{p-n}.\end{aligned}$$

Therefore,

$$\begin{aligned}(A+B)^{p+1} &= \sum_{n=0}^{p} q^{p-n}\begin{bmatrix}p\\n\end{bmatrix}_q A^{n+1}B^{p-n} + \sum_{n=0}^{p}\begin{bmatrix}p\\n\end{bmatrix}_q A^nB^{p-n+1}\\ &= \sum_{n=1}^{p+1} q^{p-n+1}\begin{bmatrix}p\\n-1\end{bmatrix}_q A^nB^{p-n+1} + \sum_{n=0}^{p}\begin{bmatrix}p\\n\end{bmatrix}_q A^nB^{p-n+1}\\ &= A^{p+1} + \left(\sum_{n=1}^{p}\left\{q^{p-n+1}\begin{bmatrix}p\\n-1\end{bmatrix}_q + \begin{bmatrix}p\\n\end{bmatrix}_q\right\}A^nB^{p-n+1}\right) + B^{p+1}\\ &= A^{p+1} + \left(\sum_{n=1}^{p}\begin{bmatrix}p+1\\n\end{bmatrix}_q A^nB^{p-n+1}\right) + B^{p+1} \quad \text{(see (5))}\\ &= \sum_{n=0}^{p+1}\begin{bmatrix}p+1\\n\end{bmatrix}_q A^nB^{p+1-n}.\end{aligned}$$

Lemma.

$$\forall k \in \mathbb{N}^*,\ (A+B)^k \equiv A^k + B^k \pmod{\Phi_k(q)\mathbf{Z}[q]}. \tag{18}$$

Proof. $q^n - 1 = \prod_{d|n}\Phi_d(q)$. Thus

$$\prod_{t=1}^{n}(q^t-1) = \prod_{d=1}^{n}(\Phi_d(q))^{[n/d]}$$

and

$$\begin{bmatrix}k\\n\end{bmatrix}_q = \prod_{d=1}^{n}(\Phi_d(q))^{[k/d]-[n/d]-[(k-n)/d]}.$$

We see that the exponent of $\Phi_k(q)$ in $[{}^k_n]_q$ is

$$\left[\frac{k}{k}\right] - \left[\frac{n}{k}\right] - \left[\frac{k-n}{k}\right] = 1 - 0 - 0 = 1, \quad \text{if } 1 \leqslant n \leqslant k-1.$$

In other terms, $\forall n \in \{1, \ldots, k-1\}$, $\Phi_k(q)$ divides $\begin{bmatrix} k \\ n \end{bmatrix}_q$, but $((\Phi_k(q))^2$ does not divide $\begin{bmatrix} k \\ n \end{bmatrix}_q$. Then (17) gives the formula to prove. □ Lemma

Proof (*continued*). Keeping the notations of Section 2, we can write

$$\forall m \in \mathbb{N}^*, (A+B)^m \equiv (A^k + B^k)^a (A+B)^b \pmod{\Phi_k(q)\mathbb{Z}[q]}.$$

Using (16), with $q = \alpha$, the kth primitive root of 1, we see that, *in this particular case*, A^k and B^k commute with any polynomial in A, B. Indeed, for instance,

$$BA^k = BAA^{k-1} = \alpha ABA^{k-1} = \alpha^2 A^2 BA^{k-2} = \cdots = \alpha^k A^k B = A^k B.$$

So

$$(A+B)^m = \left(\sum_{t=0}^{a} \binom{a}{t} A^{kt} B^{k(n-t)} \right) \left(\sum_{s=0}^{b} \begin{bmatrix} b \\ s \end{bmatrix}_\alpha A^s B^{b-s} \right). \tag{19}$$

Moreover, for the same reason, looking at the coefficient of A^n ($= A^{kc+d}$, with $0 \leqslant d < k$), we get

$$\begin{bmatrix} m \\ n \end{bmatrix}_\alpha = \binom{a}{c} \begin{bmatrix} b \\ d \end{bmatrix}_\alpha. \tag{20}$$

But, once again, since $\Phi_k(q) = \Pi_\alpha(q - \alpha)$, we see that $\mathbb{Z}[\alpha]$ is isomorphic to $\mathbb{Z}[q]/(\Phi_k(q)\mathbb{Z}[q])$, and (20) and (8) are equivalent. □

5. Applications

This noncommutative technique, and the related formulas, are useful to obtain generalizations of identities and congruences involving binomial coefficients.

Example. It is well known that

$$\forall n \in \mathbb{N}, \binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2 \tag{21}$$

and

$$\forall p \text{ (prime)}, \quad \binom{2p^k}{p^k} \equiv 2 \pmod{p^2}. \tag{22}$$

Let us try to find analogous formulas for $\begin{bmatrix} 2n \\ n \end{bmatrix}_q$. With the notations of Section 4, if $i, j \in \mathbb{N}^*$,

$$\begin{aligned} B^i A^j &= B^{i-1} BAA^{j-1} = qB^{i-1} ABA^{j-1} \\ &= qB^{i-2} BABA^{j-1} = q^2 B^{i-2} AB^2 A^{j-1} \\ &= \cdots = q^i AB^i A^{j-1}. \end{aligned}$$

Now, by induction on j, $\forall i, j \in \mathbb{N}^*$,

$$B^i A^j = q^i AB^i A^{j-1} = q^{2i} A^2 B^i A^{j-2} = \cdots$$

and

$$B^i A^j = q^{ij} A^j B^i. \tag{23}$$

That formula remains valid if i or/and j is 0. With the help of (17), the obvious identity

$$(A+B)^{2n} = (A+B)^n (A+B)^n$$

can be written

$$\begin{aligned}\sum_{k=0}^{2n} \begin{bmatrix} 2n \\ k \end{bmatrix}_q A^k B^{2n-k} &= \left(\sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q A^r B^{n-r} \right) \left(\sum_{s=0}^{n} \begin{bmatrix} n \\ s \end{bmatrix}_q A^s B^{n-s} \right) \\ &= \sum_{r=0}^{n} \sum_{s=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n \\ s \end{bmatrix}_q A^r B^{n-r} A^s B^{n-s} \\ &= \sum_{r=0}^{n} \sum_{s=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n \\ s \end{bmatrix}_q q^{s(n-r)} A^r A^s B^{n-r} B^{n-s} \quad \text{(because of (23))} \\ &= \sum_{r=0}^{n} \sum_{s=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n \\ s \end{bmatrix}_q q^{s(n-r)} A^{r+s} A^{2n-r-s}.\end{aligned}$$

Looking at the coefficient of $A^n B^n$ in each member, we get

$$\begin{bmatrix} 2n \\ n \end{bmatrix}_q = \sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n \\ n-r \end{bmatrix}_q q^{(n-r)^2}$$

and, with the symmetry (4),

$$\begin{bmatrix} 2n \\ n \end{bmatrix}_q = \sum_{r=0}^{n} q^{\binom{r}{2}} \begin{bmatrix} n \\ r \end{bmatrix}_q^2. \tag{24}$$

This is a very natural generalization of (21). Now, we have seen (see the Lemma in Section 4) that, if $1 \leqslant r \leqslant n-1$, $\Phi_n(q)$ divides $[{}^n_r]_q$. Therefore, (24) gives also

$$\begin{bmatrix} 2n \\ n \end{bmatrix}_q \equiv 1 + q^{\binom{n}{2}} \left(\mathrm{mod}\, (\Phi_n(q))^2 \mathbb{Z}[q] \right). \tag{25}$$

The special case $q = 1$ is exactly (22). Indeed,

$$\Phi_n(1) = \begin{cases} p, & \text{if } n = p^k \ (p \text{ prime}), \\ 1, & \text{otherwise,} \end{cases} \tag{26}$$

[1].

6. Remarks

- It is possible to give an identity generalizing at once (6) and Newton's formula:

$$\forall m \in \mathbb{N}^*, \sum_{n=0}^{m} \begin{bmatrix} m \\ n \end{bmatrix}_q q^{n(n-1)/2} x^n y^{m-n} = \prod_{n=0}^{m-1} (y + q^n x), \tag{27}$$

where x and y are now *commuting* variables (proof by induction).

- In the *noncommutative* algebra $\mathscr{A}$ of Section 4, we have

$$\forall m \in \mathbb{N}^*, \sum_{n=0}^{m} \binom{m}{n} q^{n(2m-n+1)/2} A^{m-n} B^n = \prod_{n-1}^{m} (A + q^n B) \tag{28}$$

(of course, proof by induction).

- Since q divides $\left[\begin{smallmatrix}2n\\n\end{smallmatrix}\right]_q - 1 - q^{(n^2)}$, (25) can be written

$$\left[\begin{matrix}2n\\n\end{matrix}\right]_q = 1 + q^{(n^2)} + q\big(\Phi_n(q)\big)^2 A_n(q), \tag{29}$$

where $A_n(q) \in \mathbb{Z}[q]$.

Moreover, $A_n(q)$ is a reciprocal polynomial, for $\left[\begin{smallmatrix}2n\\n\end{smallmatrix}\right]_q$ and $\Phi_n(q)$ are themselves reciprocal polynomials. For instance, we have

$$A_1(q) = 0,$$
$$A_2(q) = 1,$$
$$A_3(q) = q^3 + 1,$$
$$A_4(q) = q^{10} + 2q^9 + q^8 + q^7 + 2q^6 + 3q^5 + 2q^4 + q^3 + q^2 + 2q + 1,$$
$$A_5(q) = \big(q^5 + 1\big)\big(q^{10} + q^7 + q^5 + q^3 + 1\big),$$
$$\ldots$$

Of course, deg $A_n(q) = n^2 - 2 - 2\phi(n)$, where $\phi(n)$ is Euler's totient.

References

[1] S. Lang, *Algebra* (Addison-Wesley, Reading, MA, 1972).

[2] C. Radoux, Congruences entre polynômes de Gauss, Colloque de Théorie des Nombres, Univ. Valenciennes, J. Math. S.M.F.-C.N.R.S., 8 et 9 mars 1982, Société Mathématique de France.